Subject: **OTTA Leaking Sensitive Information (Advisory No 19) November, 2017**

1. **Introduction.** A report published by mobile security company Appthority reveals that enterprises are frequently **blacklisting Android and iOS application** as **they leak data and send information from device's address book to a remote server.** According to report this type of behavior pose a serious risk to enterprises when the data is sent without being encrypted. The report also enlisted top 100 Android and iOS applications along with their risk score where ***WhatsApp tops the list*.** An analysis of top **150 mobile apps found in enterprise environments showed that in the case of Android applications,** 86.7% of connections are linked to server located in the United States, followed by Ireland (7.7%), Germany (2.1%) and Sweden (0.7%). In the case of **iOS apps,** nearly 94% of connections go to servers in the United States, followed by Ireland (3.82%), the Netherlands (0.86%) and Germany (0.86%).

2. **Recommendations**

   a. Use of social media applications **especially "WhatsApp"** should be avoided as they send user information without their intervention to abroad servers.

   b. Install and UPDATE well reputed antiviruses such as Kaspersky, Bitdefender, Nod32, Avast etc.

   c. Install and regularly update software firewall such as Comodo Firewall or Zonealarm.

   d. Don't download attachments from emails unless sure about the source.